

## Dell EMC Unity Configuration Guide 4.0.1(d)

### 1) Configure Directory Services for Unity

Log into Unity with Local User

Click the “Update System Settings Widget” on the top right by the user Icon.  
Select Users and Groups

The screenshot shows the 'Settings' window of the Dell EMC Unity interface. The left sidebar contains a navigation menu with the following items: 'Software and Licenses' (selected), 'Users and Groups', 'Management', 'Storage Configuration', 'Support Configuration', 'Access', and 'Alerts'. Under 'Software and Licenses', there is a sub-menu with 'License Information' (selected), 'Software Upgrades', 'Drive Firmware', 'Language Packs', and 'System Limits'. The main content area is titled 'License Management' and contains a table with the following data:

!	License	↑	Version	Issued Date	Expire Date
✓	Antivirus Server Integration		1	9/26/2016	Permanent
✓	UnityOE V4.0		1	9/26/2016	Permanent
✓	CIFS/SMB Support		1	9/26/2016	Permanent
✓	EMC Proactive Assist		1	9/26/2016	Permanent
✓	EMC Storage Analytics (ESA)		1	9/26/2016	Permanent
✓	Fibre Channel (FC)		1	9/26/2016	Permanent
✓	File System Events Publishing		1.0	9/26/2016	Permanent
✓	Compression		1.0	9/26/2016	Permanent

Below the table, there is a section titled 'License Description' with the text: 'This license enables support for third-party antivirus solutions for your system.' At the bottom of this section, there are two buttons: 'Install License' and 'Get License Online'. At the very bottom of the window, there are two links: 'Initial Configuration Wizard' and 'Close'.

Select “Directory Services”

- Configure Distinguished Name for instance:-  
cn=Administrator,cn=Users,dc=afspc,dc=local
- LDAP Server: <THEIPADDRESSOFOYOURDIRECTORYSERVER>
- Password: The Password of the User that will connect to the Directory Server
- Port 389 (or 636 if Secure)..
- Select “Verify Connection...” and ensure a successful test

Settings

Software and Licenses

**Users and Groups**

User Management

• Directory Services

Management

Storage Configuration

Support Configuration

Access

Alerts

**Configure LDAP Server Credentials**

LDAP Domain: \* afspc.local

Distinguished Name: \* cn=Administrator,cn=Users

LDAP Server: \* 10.246.49.218

Password: \* .....

Port: 389 ☐ Use LDAPS Protocol

Advanced (Using Defaults)

Clear Configuration Upload Certificate

Verify Connection

Initial Configuration Wizard

Close Apply

Clear Configuration Upload Certificate

Verify Connection

✓ Connection Verified

Logout of the Unity Server.. and then Log Back in with an Active Directory User to verify that you can login to the system with an AD User directly the Unity User Interface (no Big-IP)

**Note: The DN that username translates to must be in the ephemeral\_LDAP\_Bypass data-group. Otherwise the PUA system will intercept the authentication and generate an ephemeral credential and the authentication will fail. This data group is under iRules/DataGroup List**

Local Traffic » iRules : Data Group List » ephemeral\_LDAP\_Bypass

⚙️ Properties

**General Properties**

Name	ephemeral_LDAP_Bypass
Partition / Path	Common
Type	String

**Records**

String Records

String:   
Value:   
Add  

cn=Administrator,cn=Users,dc=afspc,dc=local  
cn=administrator,cn=users,dc=mydomain,dc=local  
cn=f5 service account,cn=users,dc=mydomain,dc=local  
cn=proxyuser,cn=users,dc=mydomain,dc=local  
cn=testuser,cn=users,dc=afspc,dc=local

Edit Delete Record

Update Delete Data Group

## 2) Create an SSO Configuration for Unity

### A. Create a single sign on policy for Unity.

- Go to Access/Single Sign-On/Forms – Client Initiated
- Provide A name Under “SSO Configuration Name”

**Create New Forms-Client Initiated Configuration** ✕

General Settings  
Form Settings  
Header Settings

SSO Configuration Name\*:  
unity-ci1

SSO Description :

Log Setting :  
From Access Profile ▼ Create

☐ Passthrough Configuration

OK Cancel

- Click Form Settings
  - Click Create
- Provide a Form Name “frm1”
  - Click “Request Detection”
    - Detect Request form by URI
    - Request URI: /cas/login
    - Request Method GET
    - Request Prefix needs to be “checked”

**Edit Form Definition**

- Form Settings
- Request Detection**
- Form Identification
- Form Parameters
- Form Submit Detecti...
- Logon Detection
- Advanced Settings
- Javascript Injection

Detect request for form by: **URI**

Request URI\*:  
/cas/login

**Advanced Settings**

Request Method :  
**GET**

☐ Request Negative

☒ Request Prefix

OK Cancel

- Click on Form Parameters
  - Associated Form Parameters with APM Form Parameter Values.
    - Parameter Name:- password
    - Form Parameter Value: - %{session.sso.token.last.password}
    - Secure: Yes
    - Form Parameter Name:- username
    - Form Parameter Value:- %{session.sso.token.last.username}
    - Secure: No

**Edit Form Definition** [X]

- Form Settings
- Request Detection
- Form Identification
- Form Parameters**
- Form Submit Detection
- Logon Detection
- Advanced Settings
- Javascript Injection

Form Parameters

Create

<input type="checkbox"/>	Form Parameter Name	Form Parameter Value	Secure
<input checked="" type="checkbox"/>	password	%{session.sso.token.last.pass...}	true
<input type="checkbox"/>	username	%{session.sso.token.last.user...}	

Edit Delete

OK Cancel

- Form Submit Detection
  - Disable Auto detect submit:NO
  - Submit Request Prefix "Checked"

Edit Form Definiton

Form Settings

Request Detection

Form Identification

Form Parameters

Form Submit Detecti...

Logon Detection

Advanced Settings

Javascript Injection

Disable Auto detect submit :  
No

Scheme: URI

URI\*:

Advanced Settings

☐ Submit Request Negative

☒ Submit Request Prefix

OK

Cancel

- Logon Detection

# Edit Form Definiton

Form Settings

Request Detection

Form Identification

Form Parameters

Form Submit Detecti...

Logon Detection

Advanced Settings

Javascript Injection

Detect Login by: 

None

No user configurable settings

OK

Cancel

- Click Javascript Injection
  - Click Custom
  - Enter Custom JavaScript

```
<script>

function __f5submit() {

    document.getElementById("password").value =
'#{session.custom.ephemeral.last.password_sso}';

    document.getElementById("username").value = '#{session.custom.ephemeral.upn}';

    document.getElementById("submit").click();

}
```



```
if (window.addEventListener) {  
    window.addEventListener('load',__f5submit,false);  
} else if (window.attachEvent) {  
    window.attachEvent('onload',__f5submit);  
} else {  
    window.onload=__f5submit;  
}  
  
</script>
```

### 3) Create Portal Access Resource for Unity

- In the APM menu select Connectivity / VPN : Portal Access : Portal Access Lists
  - Click Create
  - Name: Your choice “Unity” for example
  - Leave Patching to be default.
  - Application URI: Needs to be the IP or hostname of the Unity Server

General Properties

Name	Unity
Partition / Path	Common
Description	
ACL Order	1

Configuration: Basic

Match Case For Paths	Yes
Patching	Type   Full Patching <input checked="" type="checkbox"/> HTML Patching <input checked="" type="checkbox"/> JavaScript Patching <input checked="" type="checkbox"/> CSS Patching <input checked="" type="checkbox"/> Flash Patching <input type="checkbox"/> Java Patching
Publish on Webtop	<input checked="" type="checkbox"/> Enable
Link Type	Application URI
Application URI	https://10.255.174.74/

Customization Settings for English

Language	English
Caption	Unity GUI
Detailed Description	
Image	<div>Choose File   No file chosen   View/Hide</div> <div>Restore Default</div>

Update

Delete

- Create a Resource Item within the portal Access Resource.
  - For resource type use the IP Address or Host Name depending upon how you are configured in your environment.
  - The IP Address/Hostname will be the IP Address or Hostname of the back end resource. Meaning the IP Address or host name of the unity server.
  - For Link Type Select “Paths”
  - For the Paths Entry Field type /\*
  - Scheme = https
  - Compression: GZIP Compression
  - Client Cache: Default
  - SSO Configuration: unity-ci (The SSO Configuration would have been created in the previous step.

Resource Item: Advanced

Link Type	<span>Paths</span>
Destination	Type: <input type="radio"/> Host Name <input checked="" type="radio"/> IP Address IP Address <input type="text" value="10.255.174.74"/>
Paths	<input type="text" value="/"/>
Scheme	<span>https</span>
Port	<input type="text" value="443"/>
Headers	Name <input type="text"/> Value <input type="text"/> Add <div></div> Edit Delete

Resource Item Properties: Advanced

Compression	<span>GZIP Compression</span>
Client Cache	<span>Default</span>
SSO Configuration	<span>unity-ci</span>
Session Update	<input checked="" type="checkbox"/> Enabled
Session Timeout	<input checked="" type="checkbox"/> Enabled
Home Tab	<input checked="" type="checkbox"/> Enabled
Log	<span>None</span>

Resource Items				Change Order...	Add...
<input checked="" type="checkbox"/>	Host or IP Address	Port	Paths		
<input type="checkbox"/>	10.255.174.74	443	/		

4) You can then associate the portal access resource item with the Webtop Policy.

- Click Access/Profiles
- Click “Edit” under Per-Session Policy
- Select the Webtop. This will be associated with an “Advanced Resource Assign Webtop Item”
- Then Select the Add/Delete Button
- Then select the Portal Access Tab
- Then Select the Portal Access webtop Item that you want to display on the webtop... for Example. “Unity”

